ECS Configuration Change Request

1. Originator	2. Log Date:	3. CCR #:	4. Rev:	5. Tel:	6. Rm #:	7. Dept.
Henry Baez	**09/26/03**	**03-0661**	**—**	301-925-1025	2101D	Sys Eng

8. CCR Title: Install IBM sendmail binary and associate file sets in DAAC and SMC firewalls.

9. Originator Signature/Date	10. Class	11. Type:	12. Need Date: 10/3/03
Henry Baez /s/ 09/26/03	**II**	**CCR**	

13. Office Manager Signature/Date	14. Category of Change:	15. Priority: (If "Emergency" fill in Block 27).
Carolyn Whitaker /s/ 09/26/03	Initial ECS Baseline Doc.	Emergency

16. Documentation/Drawings Impacted *(Review and submit checklist):*	17. Schedule Impact:	18. CI(s) Affected:
Documentation updates to follow later.		

19. Release Affected by this Change:	20. Date due to Customer:	21. Estimated Cost:
6A		None - Under 100K

22. Source Reference: ☐NCR (attach) ☐Action Item ☐Tech Ref. ☐GSFC ☐Other:

23. Problem: (use additional Sheets if necessary)

Sendmail contains a buffer overflow in the prescan() function responsible for parsing an email address. By sending a specially crafted email message it is possible to overwrite the stack or heap structures used by the sendmail process. This can allow a remote attacker to execute arbitrary code with the privileges of the sendmail daemon (typically root). Multiple attack vectors can be used to exploit this flaw. Note that since the overflow is triggered by a malicious email message, MTAs not directly facing the Internet are also at risk. This is explained more in CERT Advisory and Vulnerability Note CA-2003-25.

24. Proposed Solution: (use additional sheets if necessary)

IBM has put out a quick fix for our version of OS, AIX 4.3.3. The official fix is APAR number IY48659 will be issued sometime in October. But the problem is classified as critical so it is highly recommended the program does not wait until an unknown October date. IBM states that one OS file set also needed to be upgraded, however we found you need to install three file sets in order to make the sendmail fix work. All IBM file sets and sendmail binary have been install in VATC and PVC without any problems. The tar file is call IBMsendmailfix.tar: 'sum' 26510 30940; 'cksum' 1585119774 15841280. This release as TE.

25. Alternate Solution: (use additional sheets if necessary)

None.

26. Consequences if Change(s) are not approved: (use additional sheets if necessary)

We do not actually run IBM sendmail server on firewall, we ran a proxy called smwrap. But we do run the client and as smwrap hands the email over to delivery to sendmail, sendmail has to be fixed to protect internal sendmail servers.

27. Justification for Emergency (If Block 15 is "Emergency"):

According to advisory, if exploited this could case major disruption of email services. If internal servers is compromise, a major incidence to the program could affect a compromise site.

28. Site(s) Affected: ☐EDF ☐PVC ☐VATC ☒EDC ☒GSFC ☒LaRC ☒NSIDC ☒SMC ☐AK ☐JPL ☐EOC ☐IDG Test Cell ☐Other

29. Board Comments:	30. Work Assigned To:	31. CCR Closed Date:

32. EDF/SCDV CCB Chair (Sign/Date): **Byron Peters /s/ 10/02/03**	**Disposition:** Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ECS
33. M&O CCB Chair (Sign/Date):	**Disposition:** Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ECS
34. ECS CCB Chair (Sign/Date):	**Disposition:** Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ESDIS

ADDITIONAL SHEET

CCR #: 03-0661 Rev: — Originator: Henry Baez

Telephone: 301-925-1025 **Office:** 2101D

Title of Change: Install IBM sendmail binary and associate filesets in DAAC and SMC firewalls.

See attachmented install instructions for files sets and sendmail fix.